UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. CAMERON JOHN WAGENIUS, Defendant.	NO. CR25-142 KKE **INFORMATION**

The Acting United States Attorney charges that:

COUNT 1

(Wire Fraud Conspiracy)

Introduction

1. Defendant CAMERON JOHN WAGENIUS conspired with other persons to defraud at least 10 victim organizations by obtaining login credentials for the organizations' protected computer networks without authorization, gaining unlawful access to these protected computer networks, stealing sensitive information, threatening to leak the stolen data unless the victims paid ransoms, and offering to sell and selling the stolen data online. WAGENIUS and his co-conspirators gained unlawful access to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

hundreds of thousands of sensitive business and customer records, including non-content call and text history records, telecommunication identifying information, and other personally identifiable information.

2. WAGENIUS and his co-conspirators agreed to, attempted to, and did profit from this scheme through several means, including by attempting to extort at least $1,000,000 from victim data owners, offering to sell victims' stolen data via online messages and via posts on cybercriminal forums for thousands of dollars, successfully selling at least some of this stolen data, and using stolen victim data in further frauds, including SIM-swapping.

Relevant Individuals and Entities

3. CAMERON JOHN WAGENIUS resided in Fort Cavazos, Texas, and at a United States military base in the Republic of Korea. WAGENIUS used online accounts associated with particular nicknames, including, but not limited to, "kiberphant0m," "cyb3rph4nt0m," and "buttholio."

4. Co-Conspirator-1 resided in the Western District of Washington and used online accounts associated with particular nicknames known to the United States.

5. Co-Conspirator-2 resided in Canada and used online accounts associated with particular nicknames known to the United States.

6. Co-Conspirator-3 resided in a place unknown and used online accounts associated with particular nicknames known to the United States.

7. Victim-1 was a telecommunications company located overseas.

8. Victim-2 was a telecommunications company located in the United States.

9. Victim-3 was a technology company located in the United States. Some of Victim-2's stolen data was hosted on Victim-3's computer systems in the United States.

10. Victim-4 was a telecommunications company located in the United States.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The Conspiracy

11. Beginning on a date unknown, but no later than in or about April 2023, and continuing through at least December 18, 2024, in King County, within the Western District of Washington, and elsewhere, CAMERON JOHN WAGENIUS and others known and unknown to the United States, did knowingly agree to devise, and attempt to devise, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause to be transmitted by means of wire communication in interstate commerce writings, signs, signals, pictures, and sounds for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

Goal of the Conspiracy

12. It was the goal of the conspiracy for WAGENIUS and his co-conspirators to defraud corporations and enrich themselves by: (a) acquiring active, valid user credentials to victims' computer systems; (b) pretending to be legitimate users of these victims' networks by using those credentials to access victim computers; (c) stealing sensitive personally identifying, financial, and other valuable information from those computers; (d) threatening to leak the stolen data unless the victims paid ransoms; and (e) offering to sell the stolen data online to other criminals and foreign actors, including at least one foreign intelligence service.

Manner and Means of the Conspiracy

13. The manner and means by which WAGENIUS and his co-conspirators carried out the conspiracy included, but were not limited to, the following:

14. WAGENIUS and his co-conspirators unlawfully obtained login credentials that could be used to access the protected computer systems of victim organizations and their users, including Victims 1 through 4. They obtained these credentials using a hacking tool called "SSH Brute," among other means.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

15. WAGENIUS and his co-conspirators shared these stolen login credentials among themselves and with others, in order to access victim computer systems without authorization. To do so efficiently, they created Telegram group conversations that either manually or automatically forwarded stolen login credentials to other group members, including Co-Conspirator-1, Co-Conspirator-2, and Co-Conspirator-3. For example:

a. From at least on or about April 23, 2023, until at least June 16, 2023, WAGENIUS, Co-Conspirator-1, and others participated in a Telegram group chat. The chat members repeatedly discussed stealing computer credentials, including through brute force attacks used to guess username and password combinations, and transferred stolen credentials among themselves.

b. On or about May 19, 2024, WAGENIUS and Co-Conspirator-1 started a Telegram chat titled "SSHBRUTE," which they again used to discuss and transfer stolen credentials.

c. Between on or about June 13, 2024, and at least on or about November 17, 2024, WAGENIUS and Co-Conspirator-1 administered a second Telegram chat group in which participants, including WAGENIUS, Co-Conspirator-1, Co-Conspirator-2, and Co-Conspirator-3, exchanged hundreds of credentials. On or about June 13, 2024, Co-Conspirator-1 discussed one of these credentials. He stated, "[t]his can be pivoted from," meaning that co-conspirators could use the credentials to access a server and then "pivot" to other protected computers on the victim's computer network or steal additional data.

d. On or about September 13, 2024, WAGENIUS and Co-Conspirator-2 discussed a set of stolen credentials for a foreign telecommunications provider. Co-Conspirator-2 directed WAGENIUS to add the account to "SSH bruter."

16. WAGENIUS and his co-conspirators used these stolen credentials to unlawfully access victims' computer systems, and to view and download hundreds of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

thousands of sensitive business and customer records, including non-content call and text history records, telecommunication identifying information, and other personally identifiable information. For example:

a. In or about May 2024, WAGENIUS and Co-Conspirator-1 accessed the computer systems of Victim-1 and stole information pertaining to hundreds of thousands of Victim-1's customers.

b. In or about August and September 2024, WAGENIUS, Co-Conspirator-2, and Co-Conspirator-3 accessed the protected computer systems of Victim-3 and stole information pertaining to thousands of Victim-2's customers.

17. WAGENIUS and others publicly and privately extorted victims by threatening to sell or otherwise distribute their stolen data unless the victims paid ransoms. They did so through online posts on online cybercrime forums catering to criminals, such as BreachForums and XSS.is; Telegram channels dedicated to online frauds and other cybercrimes; direct messages on Telegram; and other online platforms such as X (formerly known as Twitter). Some of these posts and messages offered to sell the data in exchange for fiat currency and cryptocurrency, while others attempted to extort the victim companies, requesting payment in order to avoid publication of the stolen data. Some posts also published sample data stolen from the victims. The platforms on which these posts were made could be accessed from computers located anywhere in the world, including in the Western District of Washington. For example:

a. On or about May 23, 2024, WAGENIUS sent a Telegram message to another Telegram account containing the text of a ransom note addressed to Victim-1, which demanded a "ransom payment of 500,000 USD in the form of crypto currency."

b. On or about May 27, 2024, WAGENIUS posted on XSS.is an offer to sell over 250 gigabytes of information stolen from Victim-1 and published sample

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

stolen data.

c. On or about October 12, 2024, WAGENIUS posted on XSS.is an offer to sell over 325 gigabytes of information stolen from Victim-2 for $200,000 and published sample stolen data.

d. On or about November 5, 2024, WAGENIUS made two online posts on BreachForums and in a Telegram channel, each publishing portions of Victim-2's stolen data.

e. On or about November 6, 2024, WAGENIUS sent multiple emails to Victim-4 sharing sample stolen data and threatening to leak more online unless he was paid "500k USD in the form of cryptocurrency." WAGENIUS stated, "[i]n the event of [Co-Conspirator-2's] arrest I was to takeover negotiations."

f. On or about November 13, 2024, Co-Conspirator-1 messaged WAGENIUS, "We can still make money off [Victim-1]."

All in violation of Title 18, United States Code, Section 1349.

COUNT 2

(Extortion in Relation to Computer Fraud)

18. The allegations contained in paragraphs 1 through 10 and 12 through 17 of this Information are realleged and incorporated as if fully set forth herein.

19. On or about October 22, 2024, in the Western District of Texas, and elsewhere, CAMERON JOHN WAGENIUS, with intent to extort from persons money and things of value, transmitted in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization. Specifically, WAGENIUS wrote, "If I'm not contacted all 358+ [gigabytes] of data on the [Victim-2] network will be released."

20. On or about November 5, 2024, WAGENIUS publicly posted Victim-2's stolen data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

All in violation of Title 18, United States Code, Section 1030(a)(7)(B).

COUNT 3

(Aggravated Identity Theft)

21. On or about November 5, 2024, in King County, within the Western District of Washington, and elsewhere, CAMERON JOHN WAGENIUS did knowingly transfer, possess, and use, and aided and abetted the transfer, possession, and use of, without lawful authority, the means of identification of another person, to wit, a telephone number, which belonged to a real person who was Victim-2's customer, during and in relation to the specified violations of Title 18, United States Code, Sections 1349 and 1030 that are charged above in Counts 1 and 2.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATIONS

22. The allegations contained in Counts 1–3 above are hereby realleged and incorporated by reference for the purpose of alleging forfeiture.

23. Upon conviction of the offense alleged in Count 1, CAMERON JOHN WAGENIUS shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), any property constituting, or derived from, proceeds traceable to the offense. Such property includes, but is not limited to, a judgment for a sum of money representing the amount of proceeds Defendant obtained as a result of the offense.

24. Upon conviction of the offense alleged in Count 2, CAMERON JOHN WAGENIUS shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B), and any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the offense, and, pursuant to Title 18, United States Code, Section 1030(i)(1)(A), any personal property that was used or intended to be used to commit or to facilitate the commission of the offense. Such

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

property includes, but is not limited to, a judgment for a sum of money representing the amount of proceeds Defendant obtained as a result of the offense.

25. **Substitute Assets.** If any of the above-described forfeitable property, as a result of any act or omission of the defendant,

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. it is the intent of the United States to seek the forfeiture of any other property of the defendant, up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, Section 853(p).

DATED this 14th day of July, 2025.

s/ Sarah G. Vogel, for
TEAL LUTHY MILLER
Acting United States Attorney

SOK TEA JIANG
Assistant United States Attorney
Western District of Washington

LOUISA K. BECKER
Senior Counsel
Computer Crime & Intellectual Property Section, Criminal Division, USDOJ

GEORGE BROWN
Trial Attorney
Computer Crime & Intellectual Property Section, Criminal Division, USDOJ

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970